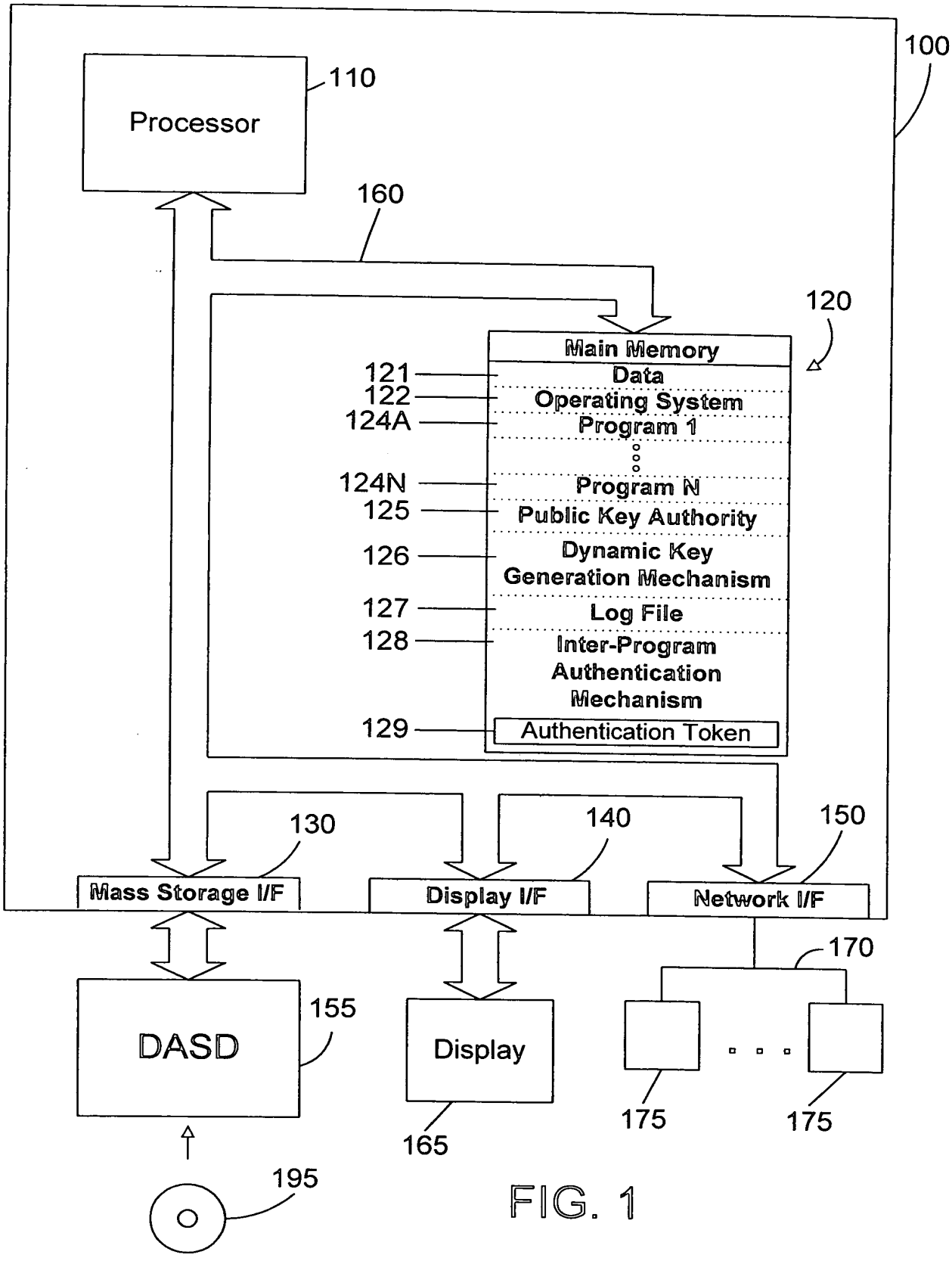
100
Processor
110
160
120
Main Memory
121
Data
122
Operating System
124A
Program 1
124N
Program N
125
Public Key Authority
126
Dynamic Key Generation Mechanism
127
Log File
128
Inter-Program Authentication Mechanism
129
Authentication Token
130
140
150
Mass Storage I/F
Display I/F
Network I/F
170
DASD
155
Display
165
175
175
195

FIG. 1

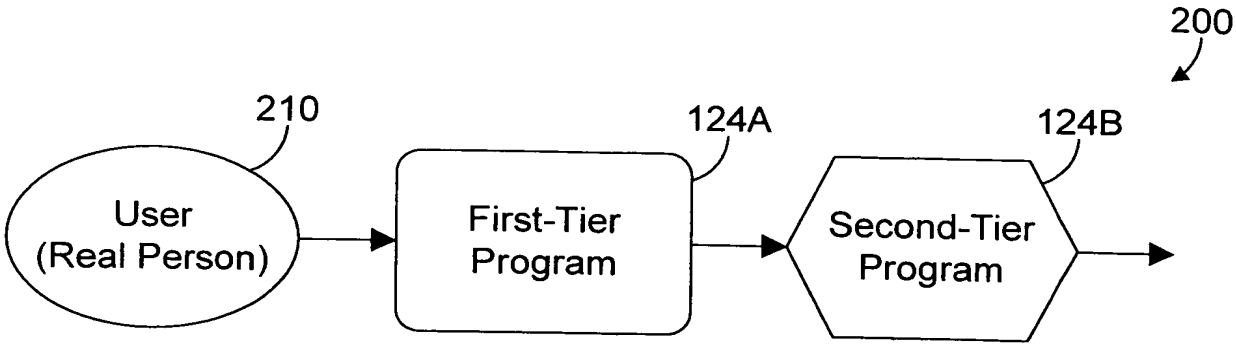

FIG. 2 Prior Art

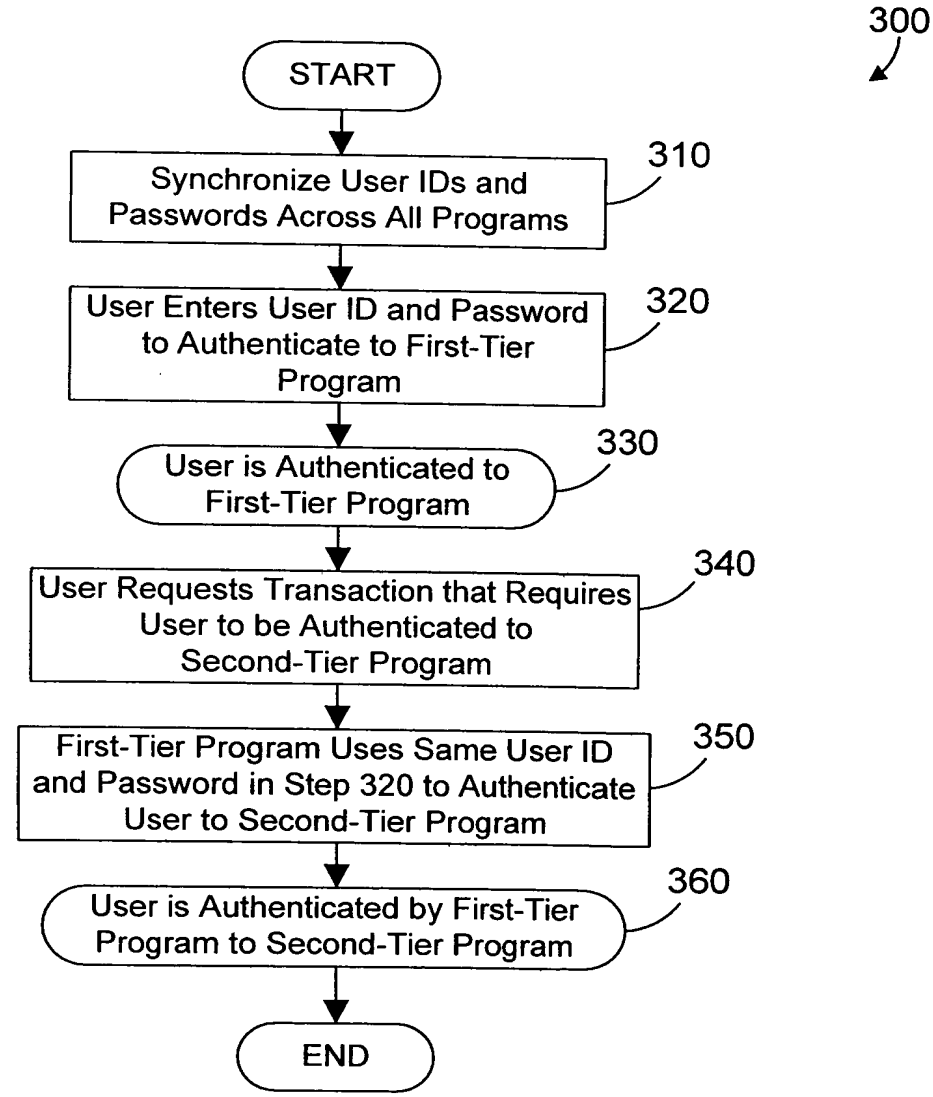

FIG. 3 Prior Art

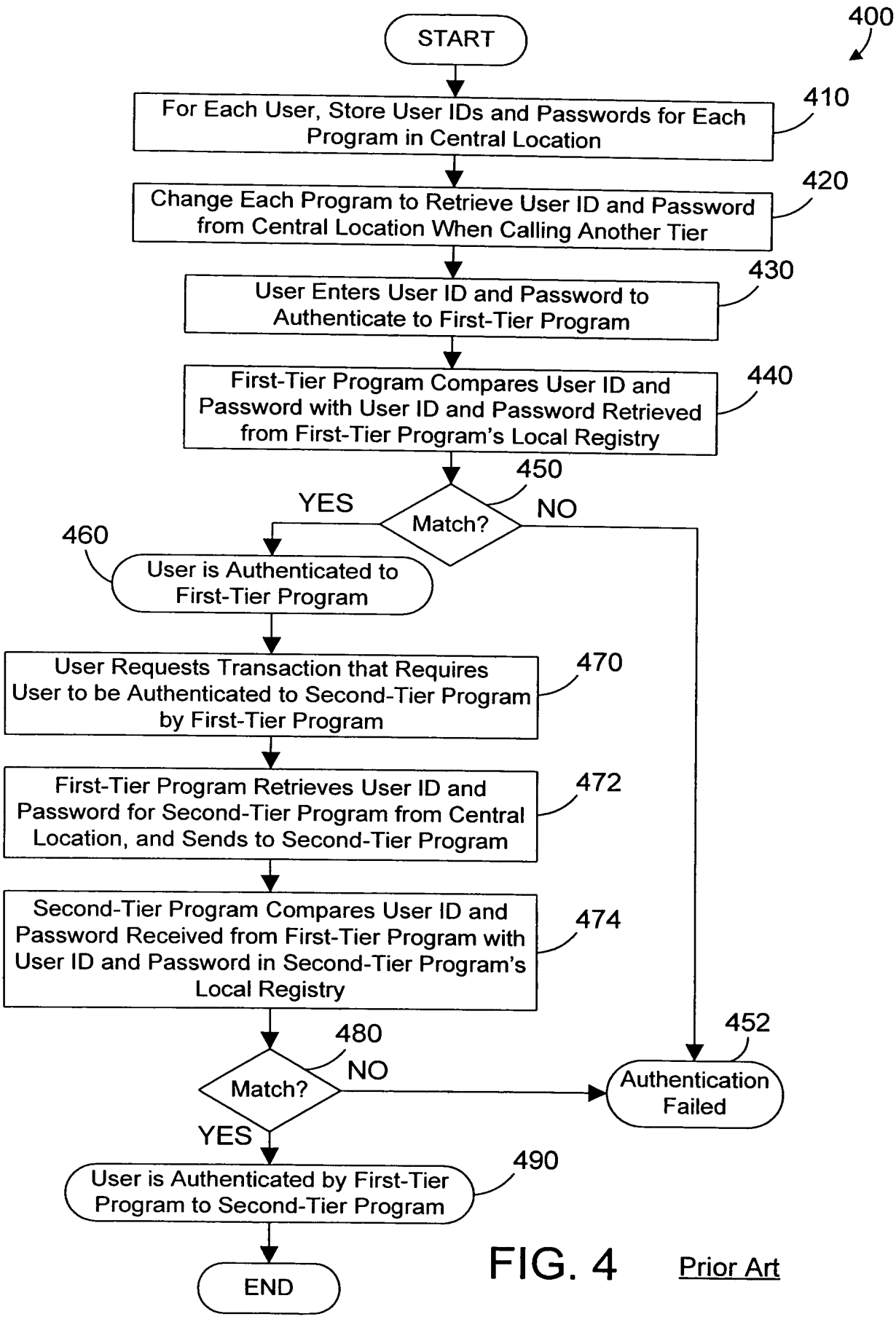

FIG. 4 Prior Art

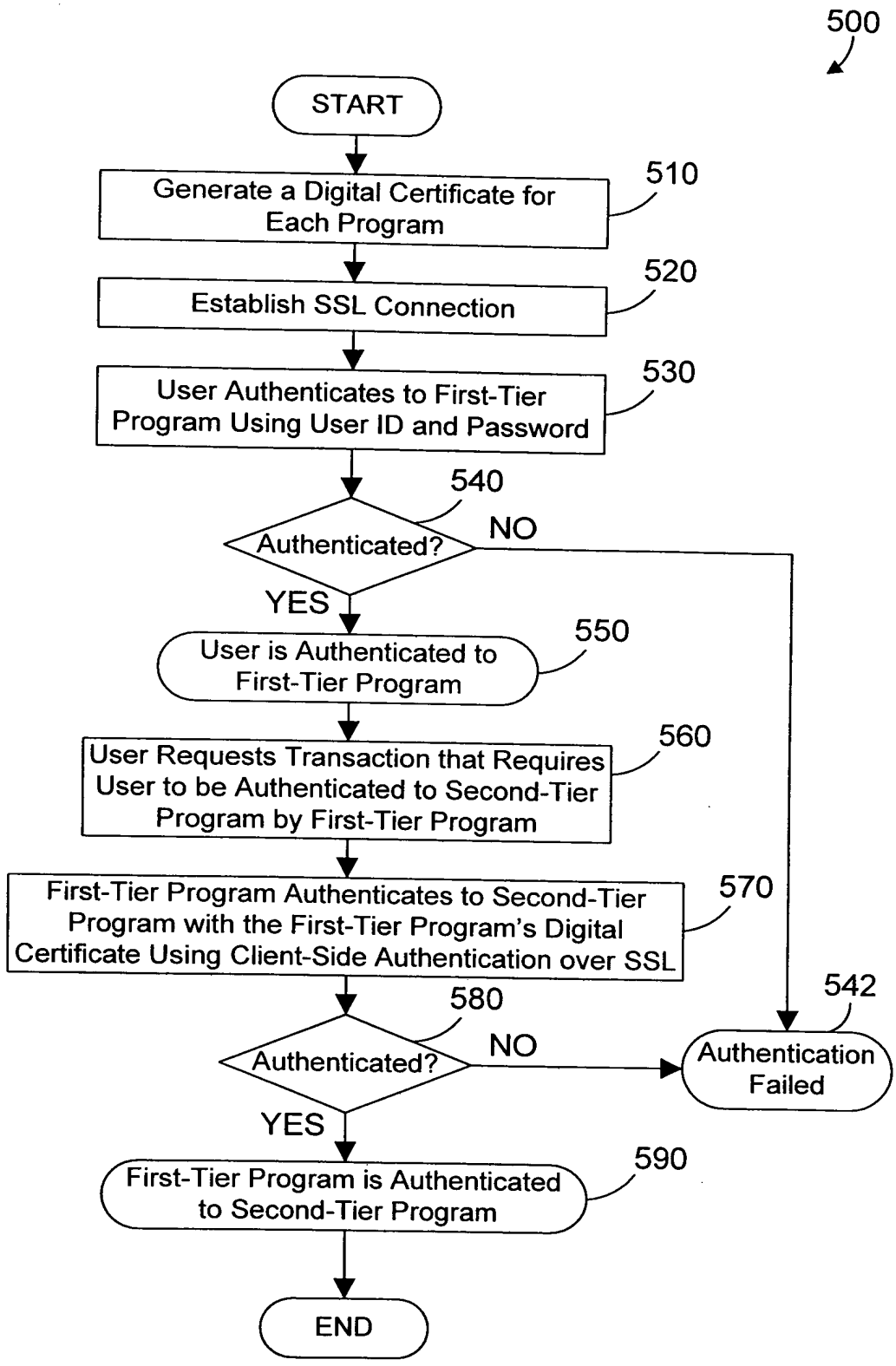

FIG. 5 Prior Art

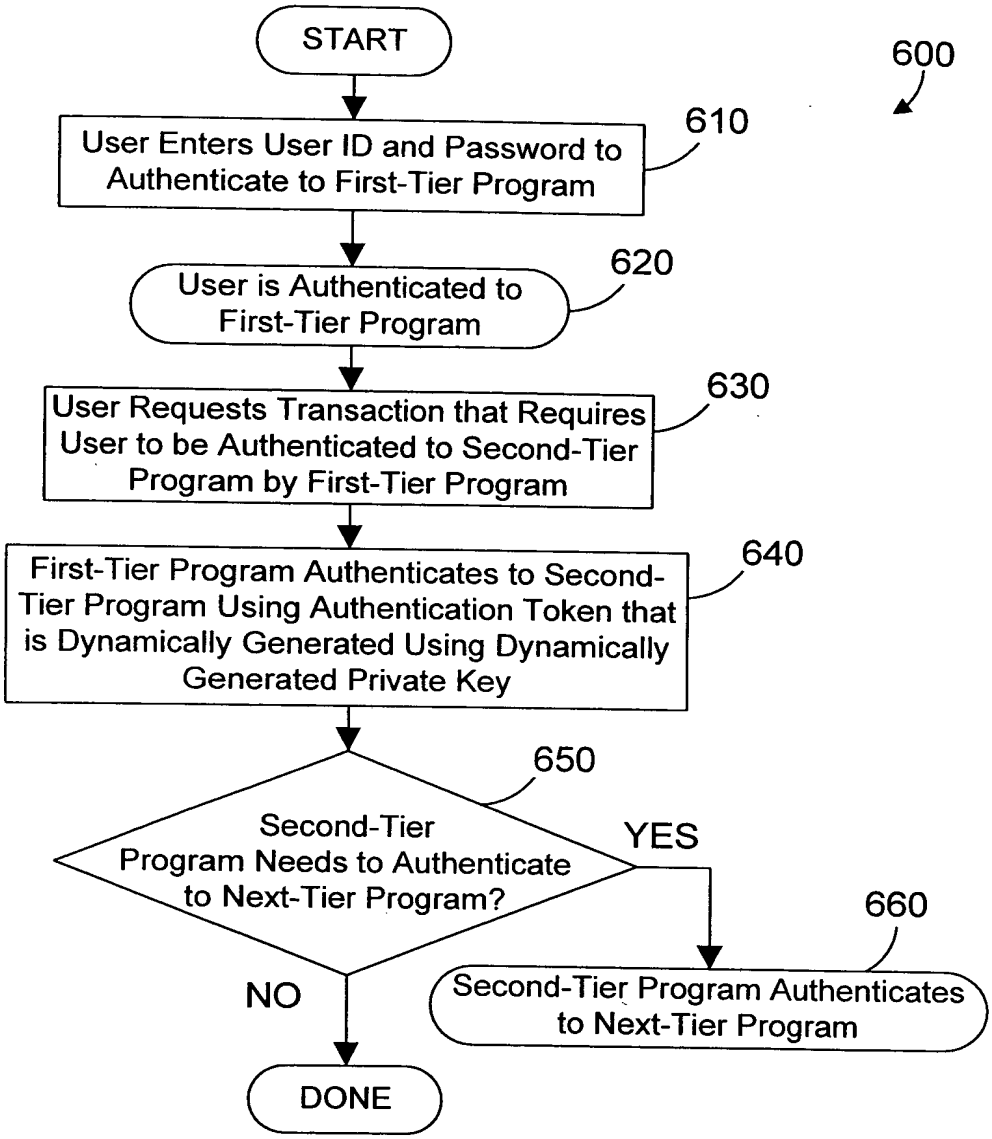
START
600
User Enters User ID and Password to Authenticate to First-Tier Program
610
User is Authenticated to First-Tier Program
620
User Requests Transaction that Requires User to be Authenticated to Second-Tier Program by First-Tier Program
630
First-Tier Program Authenticates to Second-Tier Program Using Authentication Token that is Dynamically Generated Using Dynamically Generated Private Key
640
Second-Tier Program Needs to Authenticate to Next-Tier Program?
650
YES
NO
Second-Tier Program Authenticates to Next-Tier Program
660
DONE

FIG. 6

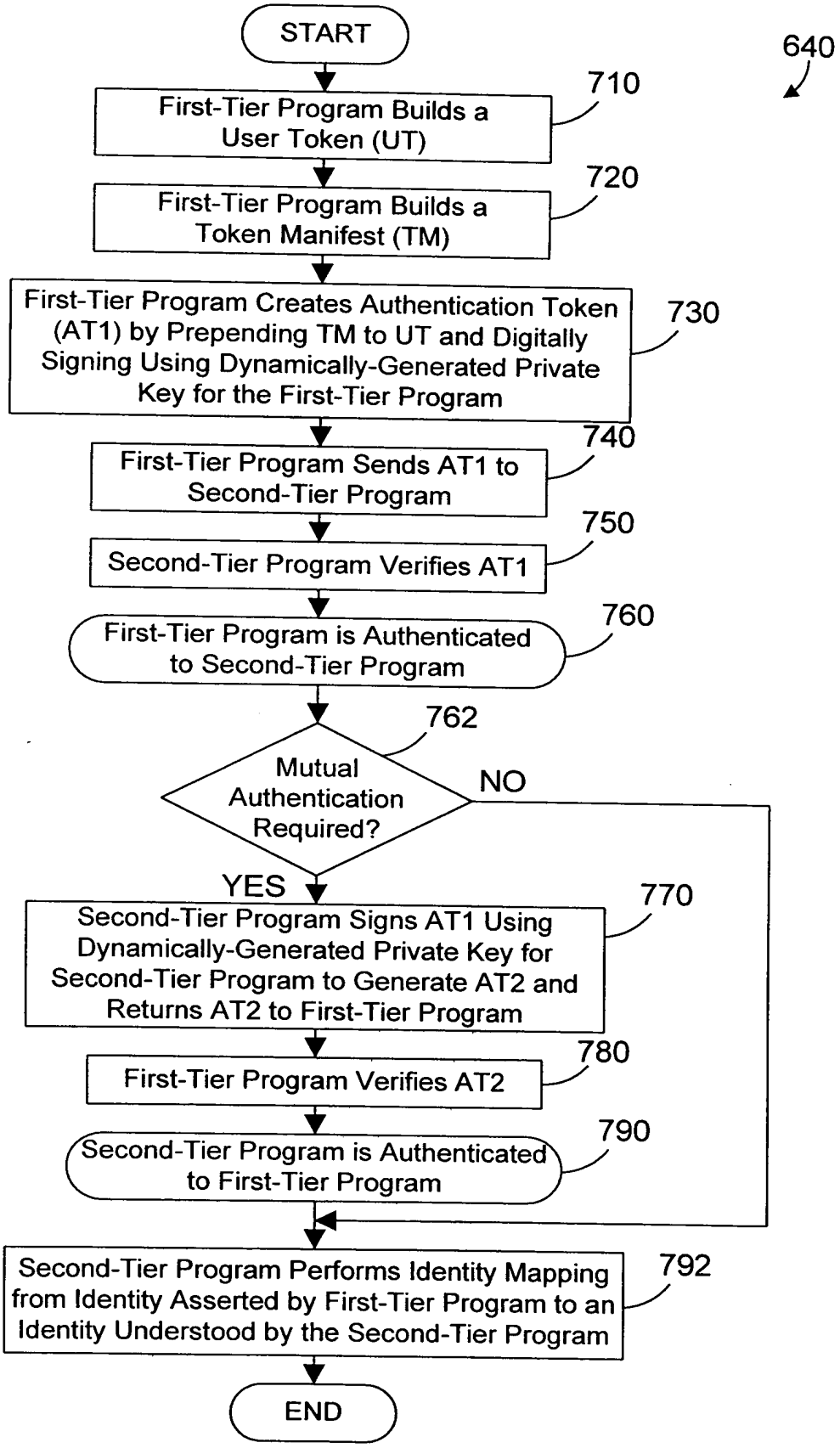
START
640
First-Tier Program Builds a User Token (UT)
710
First-Tier Program Builds a Token Manifest (TM)
720
First-Tier Program Creates Authentication Token (AT1) by Prepending TM to UT and Digitally Signing Using Dynamically-Generated Private Key for the First-Tier Program
730
First-Tier Program Sends AT1 to Second-Tier Program
740
Second-Tier Program Verifies AT1
750
First-Tier Program is Authenticated to Second-Tier Program
760
Mutual Authentication Required?
762
NO
YES
Second-Tier Program Signs AT1 Using Dynamically-Generated Private Key for Second-Tier Program to Generate AT2 and Returns AT2 to First-Tier Program
770
First-Tier Program Verifies AT2
780
Second-Tier Program is Authenticated to First-Tier Program
790
Second-Tier Program Performs Identity Mapping from Identity Asserted by First-Tier Program to an Identity Understood by the Second-Tier Program
792
END

FIG. 7

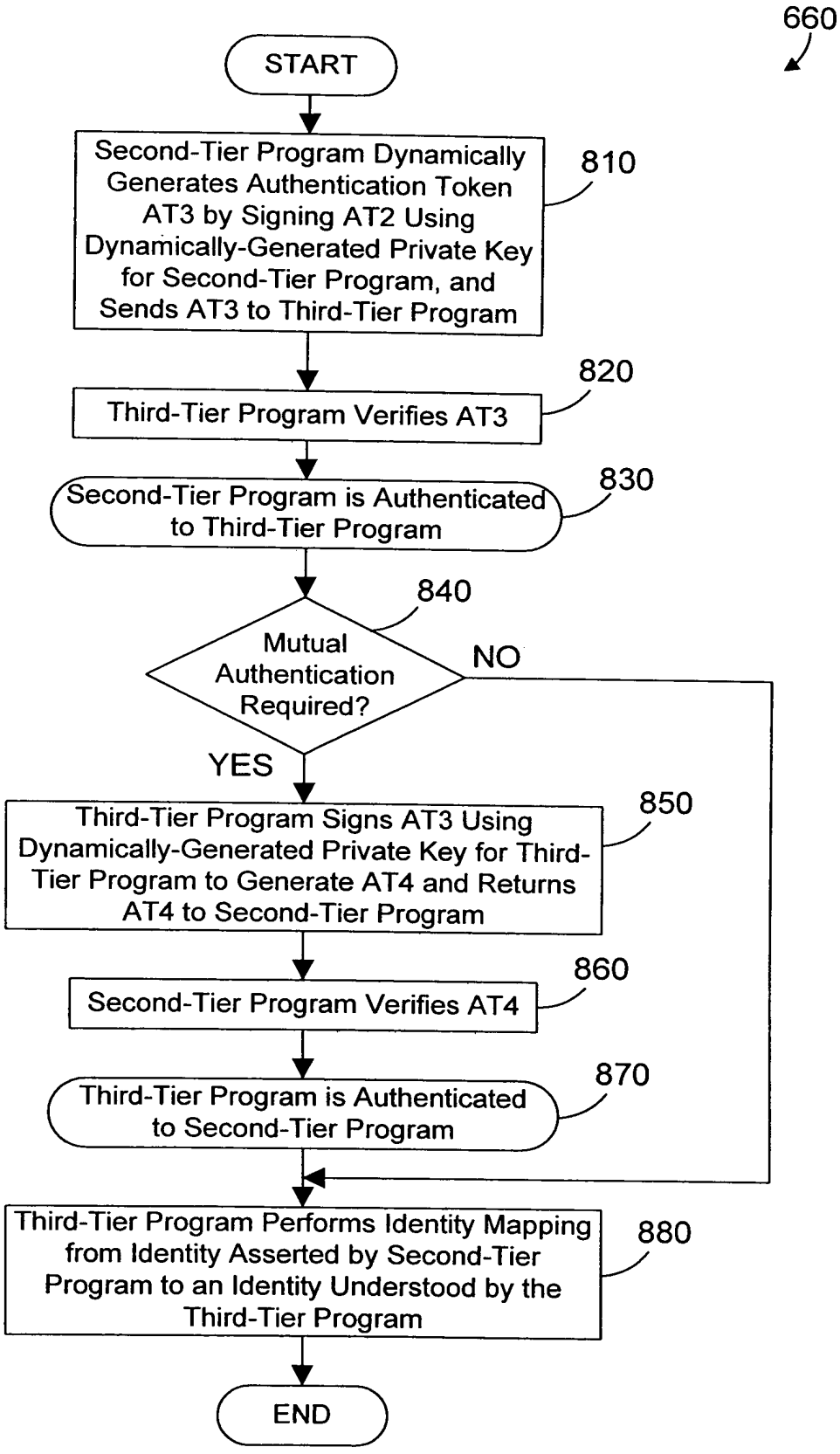
660
START
Second-Tier Program Dynamically Generates Authentication Token AT3 by Signing AT2 Using Dynamically-Generated Private Key for Second-Tier Program, and Sends AT3 to Third-Tier Program
810
Third-Tier Program Verifies AT3
820
Second-Tier Program is Authenticated to Third-Tier Program
830
Mutual Authentication Required?
840
NO
YES
Third-Tier Program Signs AT3 Using Dynamically-Generated Private Key for Third-Tier Program to Generate AT4 and Returns AT4 to Second-Tier Program
850
Second-Tier Program Verifies AT4
860
Third-Tier Program is Authenticated to Second-Tier Program
870
Third-Tier Program Performs Identity Mapping from Identity Asserted by Second-Tier Program to an Identity Understood by the Third-Tier Program
880
END

FIG. 8

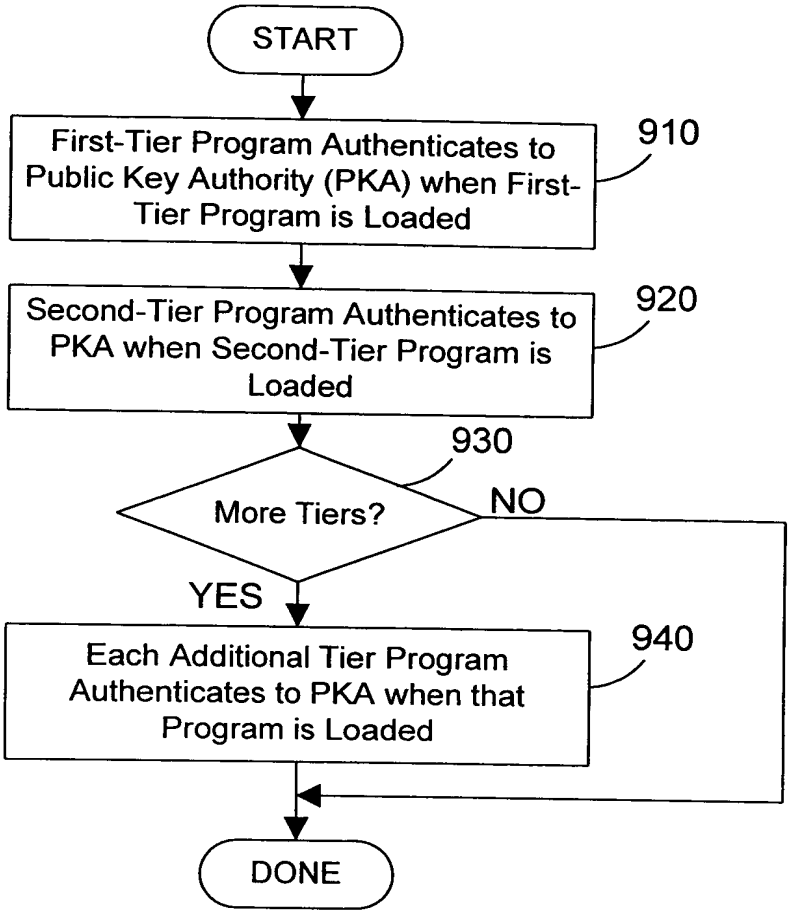
START
First-Tier Program Authenticates to Public Key Authority (PKA) when First-Tier Program is Loaded
910
900
Second-Tier Program Authenticates to PKA when Second-Tier Program is Loaded
920
930
More Tiers?
NO
YES
Each Additional Tier Program Authenticates to PKA when that Program is Loaded
940
DONE

FIG. 9

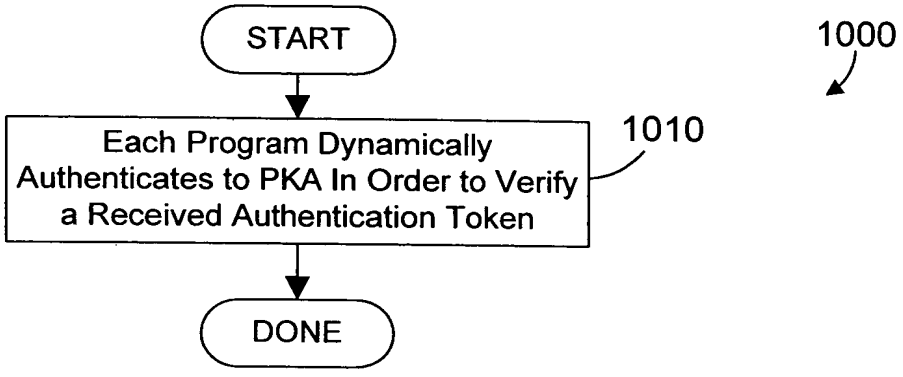
START
1000
Each Program Dynamically Authenticates to PKA In Order to Verify a Received Authentication Token
1010
DONE

FIG. 10

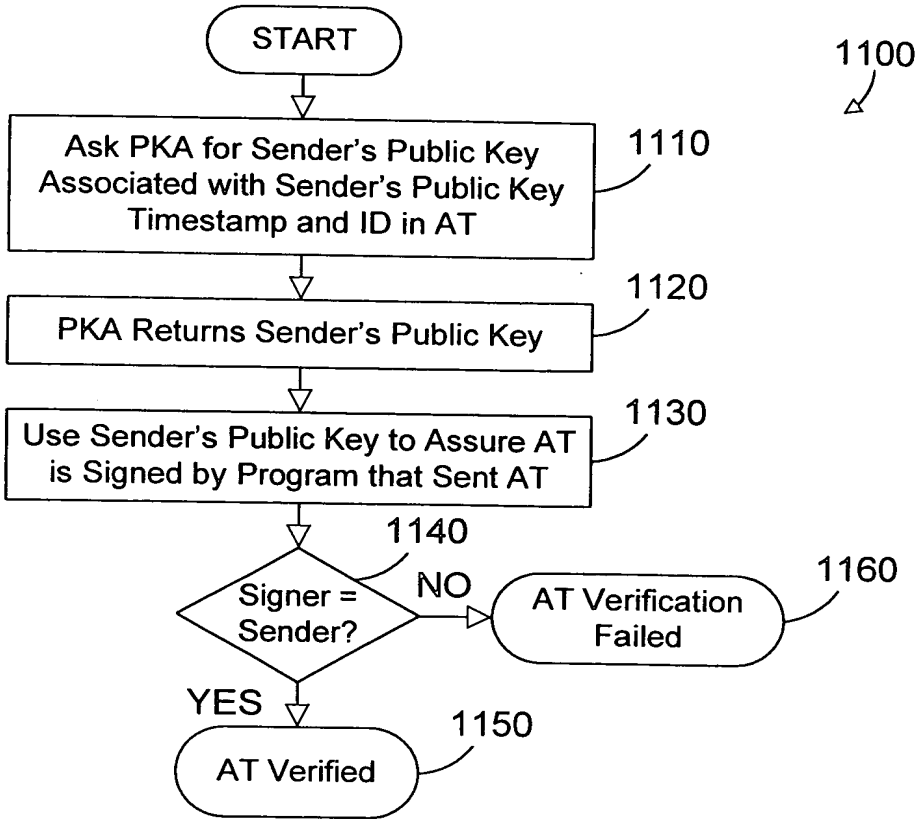
START
1100
Ask PKA for Sender's Public Key Associated with Sender's Public Key Timestamp and ID in AT
1110
PKA Returns Sender's Public Key
1120
Use Sender's Public Key to Assure AT is Signed by Program that Sent AT
1130
1140
Signer = Sender?
NO
AT Verification Failed
1160
YES
AT Verified
1150

FIG. 11

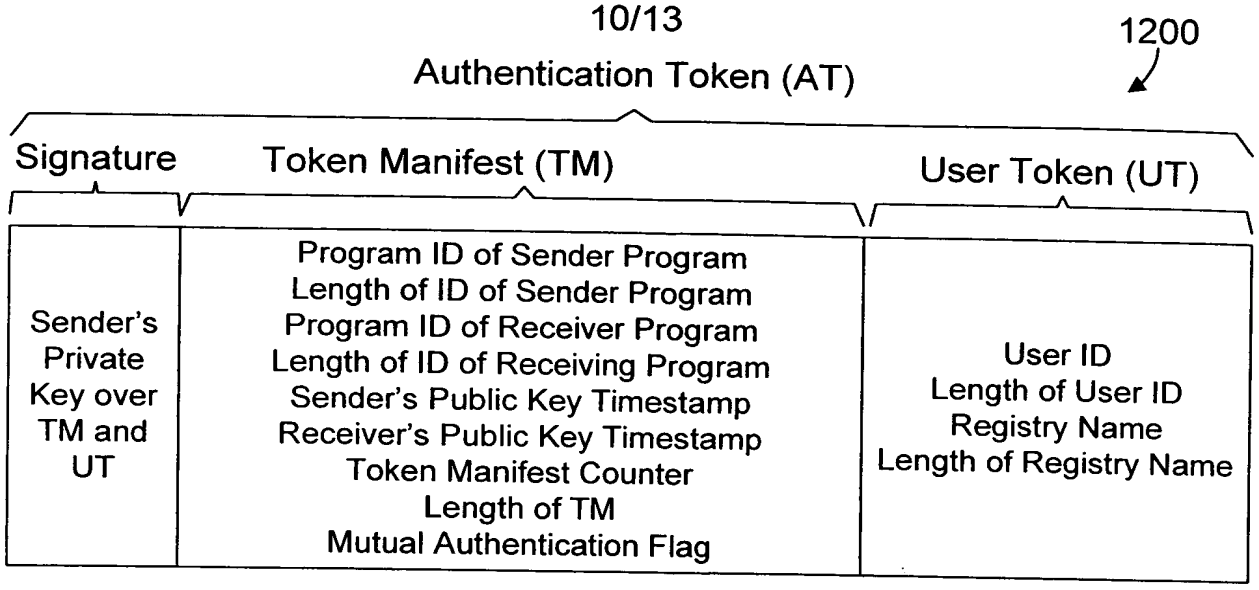

FIG. 12

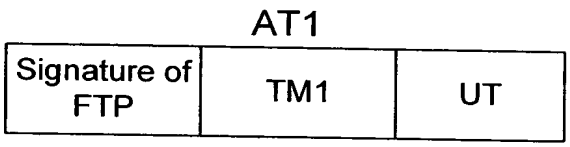

FIG. 13

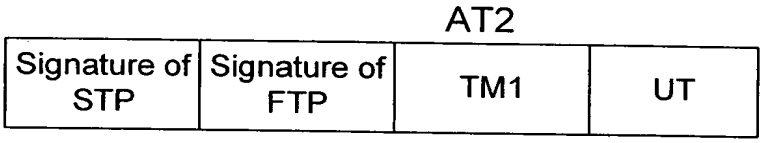

FIG. 14

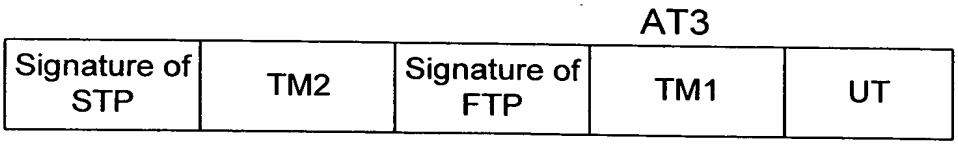

FIG. 15

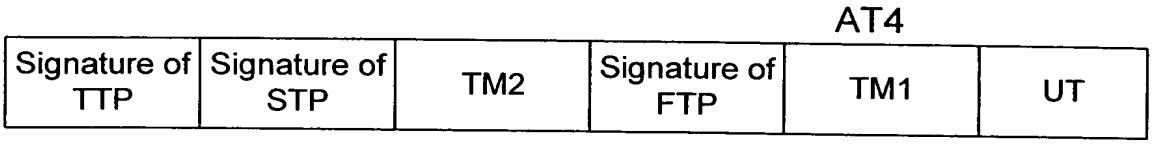

FIG. 16

AT5

Signature of TTP	TM3	Signature of STP	TM2	Signature of FTP	TM1	UT

FIG. 17

ATN

Signature of NTP	TMN	...	Signature of TTP	TM3	Signature of STP	TM2	Signature of FTP	TM1	UT

FIG. 18

AT3'

Signature of PKA	Signature of STP	TM2	Signature of FTP	TM1	UT

FIG. 19

AT5'

Signature of PKA	Signature of TTP	TM3	Signature of STP	TM2	Signature of FTP	TM1	UT

FIG. 20

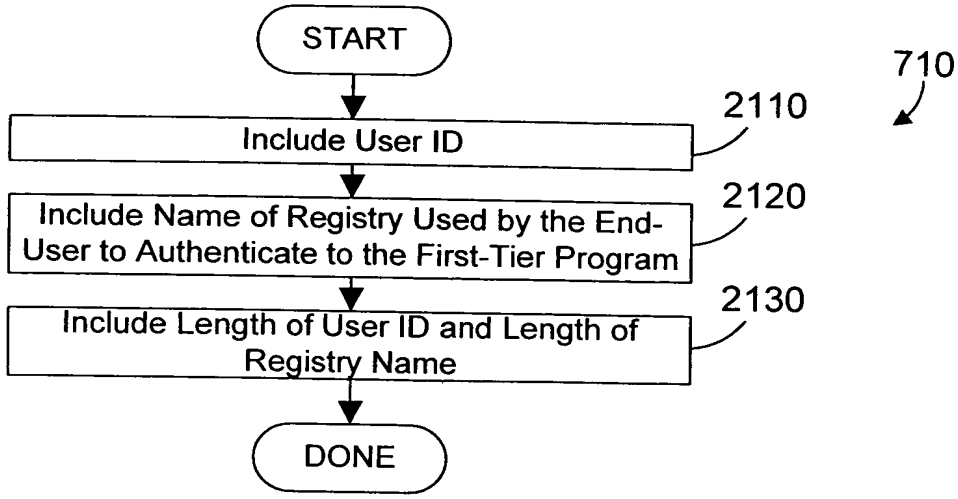
START
710
2110
Include User ID
2120
Include Name of Registry Used by the End-User to Authenticate to the First-Tier Program
2130
Include Length of User ID and Length of Registry Name
DONE

FIG. 21

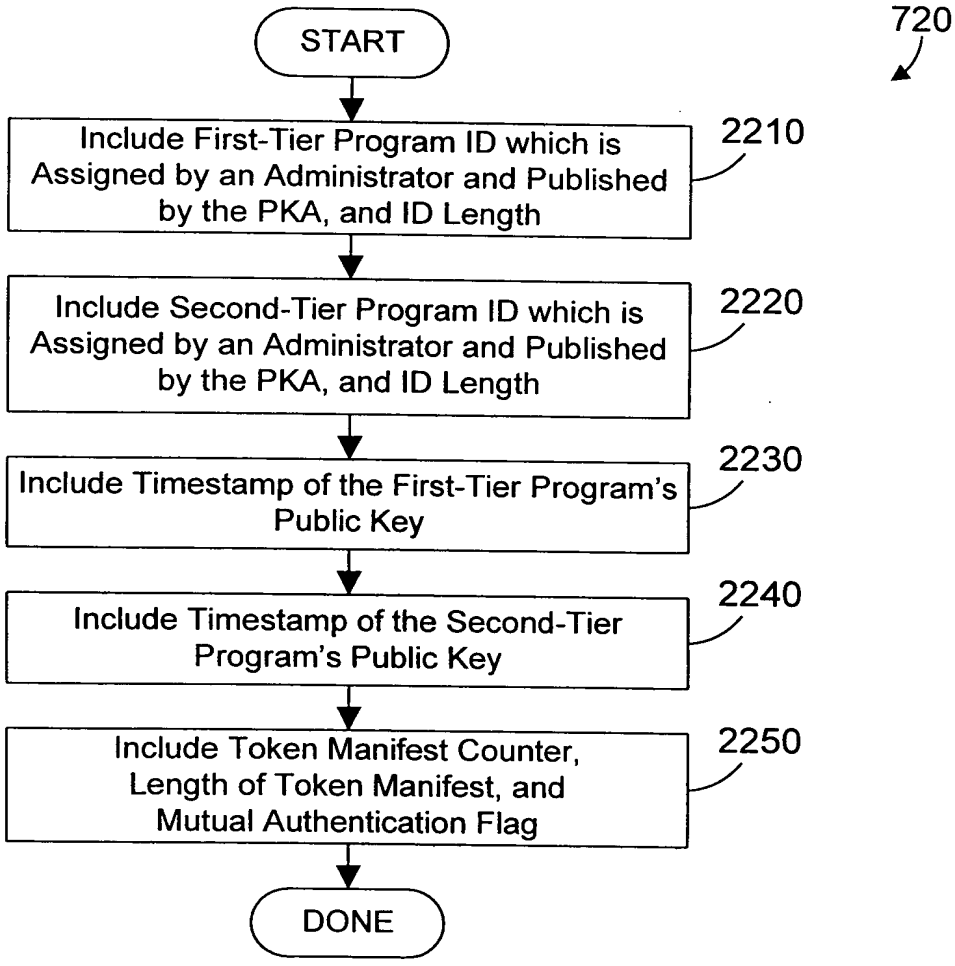
START
720
2210
Include First-Tier Program ID which is Assigned by an Administrator and Published by the PKA, and ID Length
2220
Include Second-Tier Program ID which is Assigned by an Administrator and Published by the PKA, and ID Length
2230
Include Timestamp of the First-Tier Program's Public Key
2240
Include Timestamp of the Second-Tier Program's Public Key
2250
Include Token Manifest Counter, Length of Token Manifest, and Mutual Authentication Flag
DONE

FIG. 22

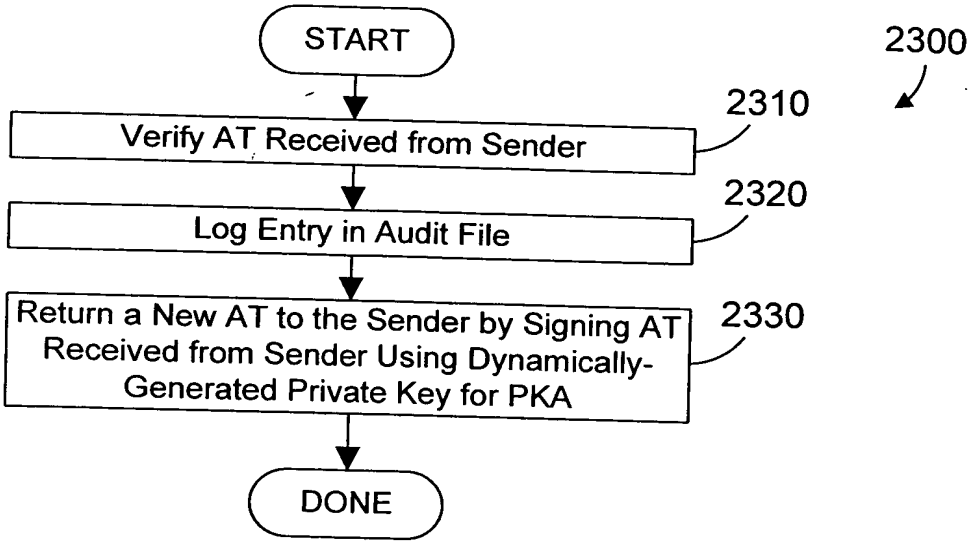
START
2300
2310
Verify AT Received from Sender
2320
Log Entry in Audit File
2330
Return a New AT to the Sender by Signing AT Received from Sender Using Dynamically-Generated Private Key for PKA
DONE

FIG. 23